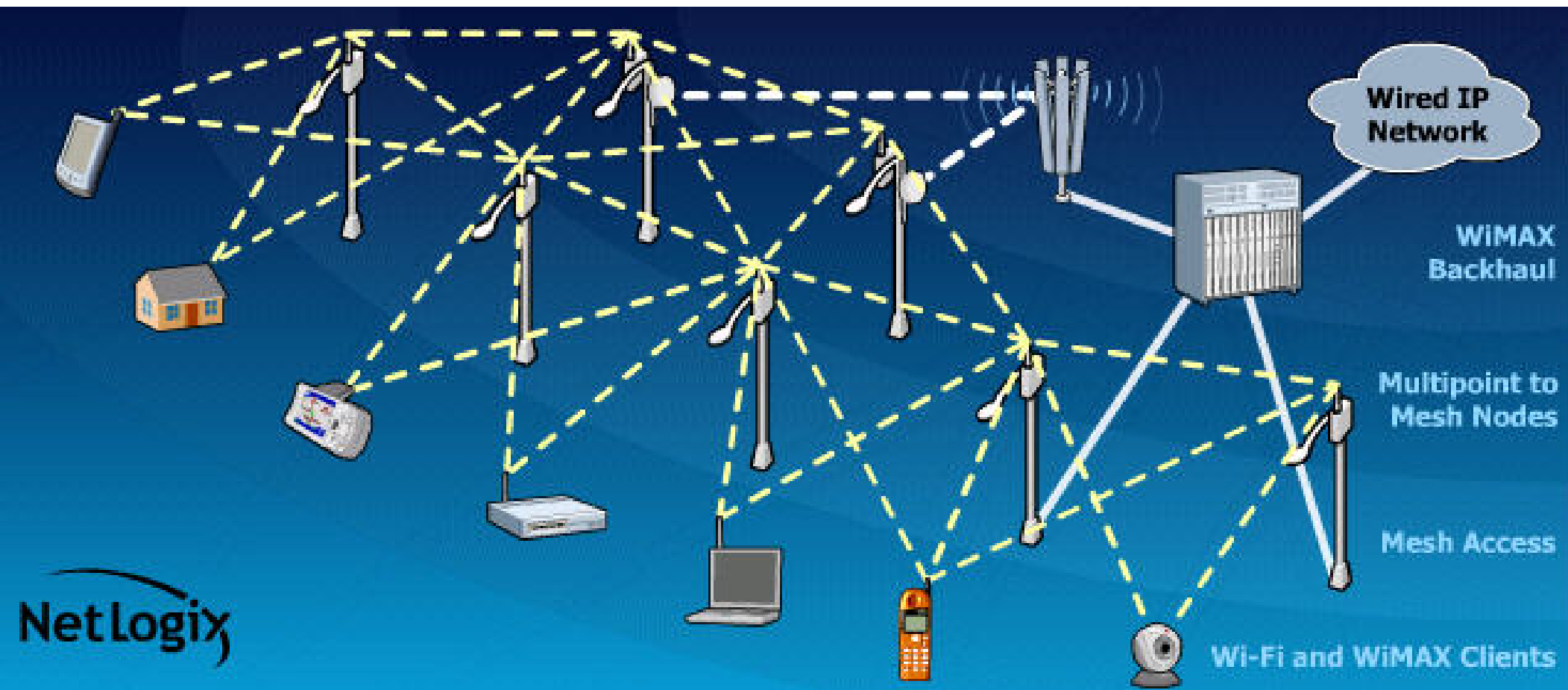


WIRELESS BROADBAND TECHNOLOGY PRIMER



Are We Talking Rocket Science?





Licensed vs. Unlicensed

Licensed

- ▶ Spectrum is expensive
- ▶ Less interference
- ▶ Longer to deploy
- ▶ More expensive equipment
- ▶ Fewer vendors to select from
- ▶ More interaction required with FCC
- ▶ FCC will respond to complaints about interference, power use, spectrum use, etc.

Unlicensed

- ▶ Spectrum is FREE
- ▶ More interference
- ▶ Fast deployment
- ▶ Less expensive equipment
- ▶ Many vendors to select from
- ▶ Little interaction with the FCC
- ▶ Response to complaints from FCC is unlikely
 - ✧ 5.4 ~ 5.7GHz just released (11 more channels for 802.11a)
 - ✧ 4.9GHz for Public Safety



Managing Interference

Anyone can use unlicensed spectrum

- ❑ The trick is managing unlicensed spectrum and interference

Managing interference is much easier with the advent of 5.4 GHz.

- ❑ More Channels
- ❑ Dynamic Frequency Selection (DFS)

Primary cause of interference is “self interference”

Incidents of interference can be reduced through:

- ▶ Solid network design
- ▶ Good vendor selection (OFDM-based equipment)
- ▶ Efficient operational procedures
 - Channel planning with local WISPs and other local unlicensed wireless networks.
 - Performance monitoring & trending
 - Etc.



Public Safety Networks: 4.9GHz

Eligibility

- ▶ All State or local entities are eligible to hold 4.9GHz licenses
- ▶ Rule went into effect January 18, 2005
- ▶ Few vendors FCC certified but many in process

Types of Uses

- ▶ Communications must be related to protection of life, liberty, or property
 - ✧ Wireless LANs for incident scene management
 - ✧ Mobile data
 - ✧ Video Security
 - ✧ VoIP
 - ✧ PDA Connectivity
 - ✧ Hot Spots (Public Safety use)
 - ✧ T1 Replacement



What Does 4.9GHz Mean?

1. Free of Interference from Public Networks
2. City can use spectrum dedicated to public safety FREE OF CHARGE
3. More Efficient Public Safety Communications



How Do You File for a 4.9GHz license?

Visit the FCC Website

or

Send us an email...we'll send the link.



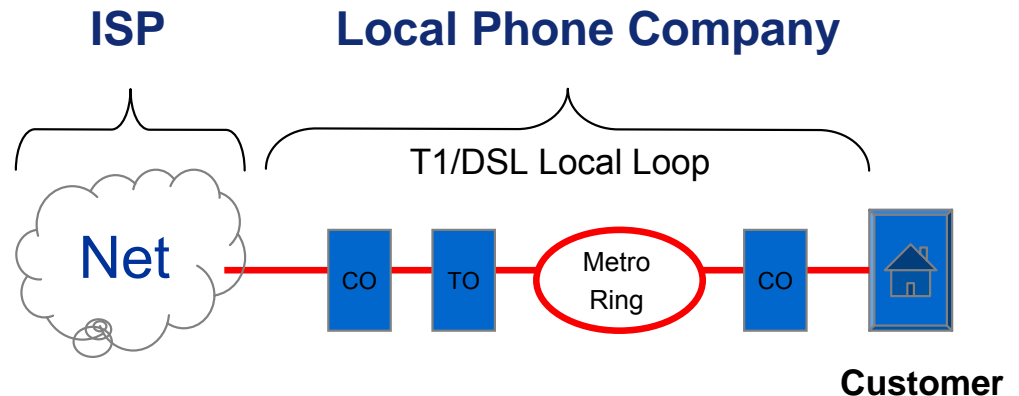
Wired vs. Wireless

- ▶ Wireless is an excellent for:
 1. Greenfield deployments (where no wired facilities exist).
 2. Deployments where upgrading wired plant is too costly.
 3. Where time to market is imperative.
 4. Mobile & Portable Applications.
 5. Wired Bypass
- ▶ Any wireless network that connects to the Internet must connect to a wired transit network connection somewhere.
- ▶ Wired and Wireless networks will continue to coexist and interconnect for the foreseeable future.
- ▶ The goal in the design and development of any network is to find the “sweet spot” for the best mix.

Broadband Wireless Advantages

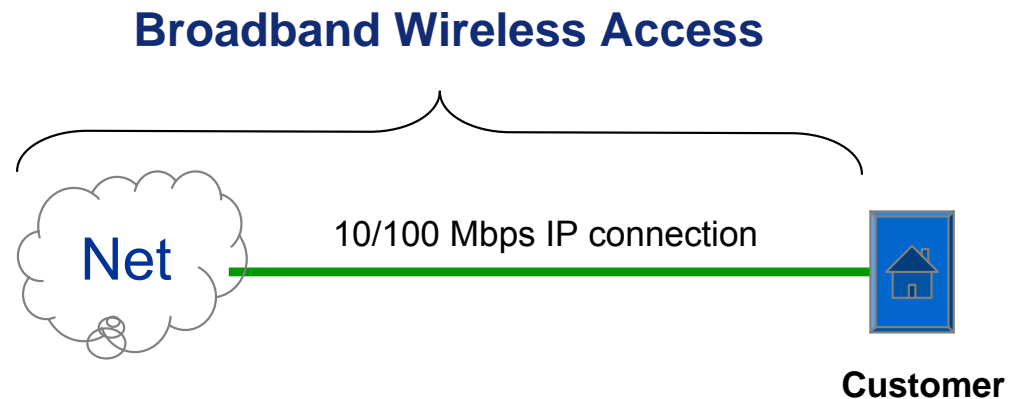
Typical Wireline Scenario

- ▶ Loop required from Telco
- ▶ Adds significant cost to service
- ▶ Lengthy install
- ▶ Not flexible



Broadband Wireless Access

- ▶ Completely on-net service
- ▶ Reduced revenue to Carrier/Telco
- ▶ Lower cost access
- ▶ Highly flexible
- ▶ More control
- ▶ Stronger ownership
- ▶ Bandwidth for new apps





Wireless Standards

- ▶ **Wi-Fi**
- ▶ **WiMAX**
- ▶ **Future Standards**



What is WiFi?

- ▶ “WiFi” is short for “Wireless Fidelity”
- ▶ It is an IEEE* 802.11 standard developed to enable “Wireless Ethernet” communications
 - ❑ The cable that connects your PC to the network is an Ethernet cable.
- ▶ WiFi was originally designed for indoor use
- ▶ Many vendors now have WiFi routers that work outdoors.
- ▶ WiFi has become so popular that 90M chips are produced monthly!
 - ❑ WiFi is standard on almost all new laptops
 - ❑ And growing rapidly! (Ex.: household appliances, RFID, etc.)

* IEEE = “Institute of Electronic and Electrical Engineers”



Common 802.11 Standards

- ▶ 802.11b
 - ❑ 11Mbps speeds
 - ❑ 2.4GHz
 - ❑ Lowest cost wireless equipment available

- ▶ 802.11g
 - ❑ 54Mbps speeds
 - ❑ 2.4GHz
 - ❑ Backwards compatible with .11b

- ▶ 802.11a
 - ❑ 54Mbps speeds
 - ❑ 5.8GHz
 - ❑ Excellent for backhaul between .11b/g nodes



WiMAX – What is it?

► 802.16

- ❑ Original spec - Designed to standardize LMDS implementations (for use above 11 GHz.)

► 802.16a

- ❑ Designed for the lower 2~11 GHz bands.
- ❑ Intended for "last mile" competition with DSL & Cable – Promoted by WiMAX Forum
- ❑ Intended to deliver up-to-70 Mbps with a range up to 30 miles.
- ❑ Uses fixed, Line-of-sight antennas.
- ❑ Doesn't include "handoff"

► 802.16d (802.16-2004)

- ❑ Consolidates previous revisions – final revision before mobility.
- ❑ Among the changes is support of MIMO antennas, which will likely increase reliable range amid multipath. It may enable easy installs with indoor antennas.

► 802.16e

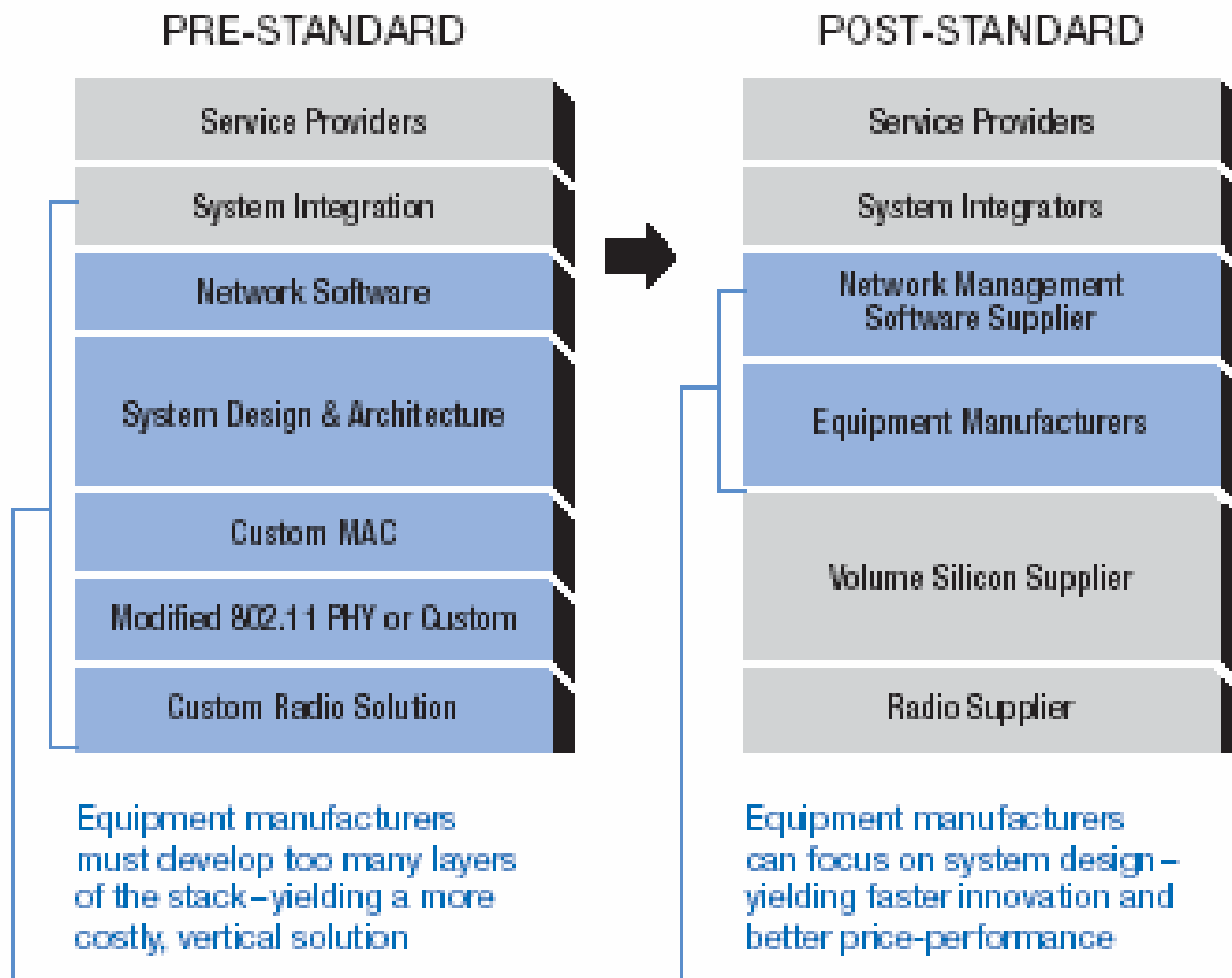
- ❑ Adds mobility features.
- ❑ Narrower bandwidth (a max of 5 MHz), slower speed and smaller antennas allow "walkabout" or vehicular mobility (up to 40mph or so).
- ❑ It's backwards compatible with the 802.16 standard.
- ❑ At 3.5 GHz & lower it may provide some competition to cellular with a range of 1-3 miles in cities.

What is WiMAX?

Summary

- ▶ Backed by Intel as an ideal backhaul for Cellular and Wi-Fi (802.11a/b/g)
- ▶ Includes QoS which allows for broadband on demand & voice packet prioritization
- ▶ Increased security
- ▶ Lower cost on equipment
- ▶ Future interoperability in mobile applications
- ▶ Intel's vested interest: *more laptop sales means more high margin business*

802.16 Industry Structure



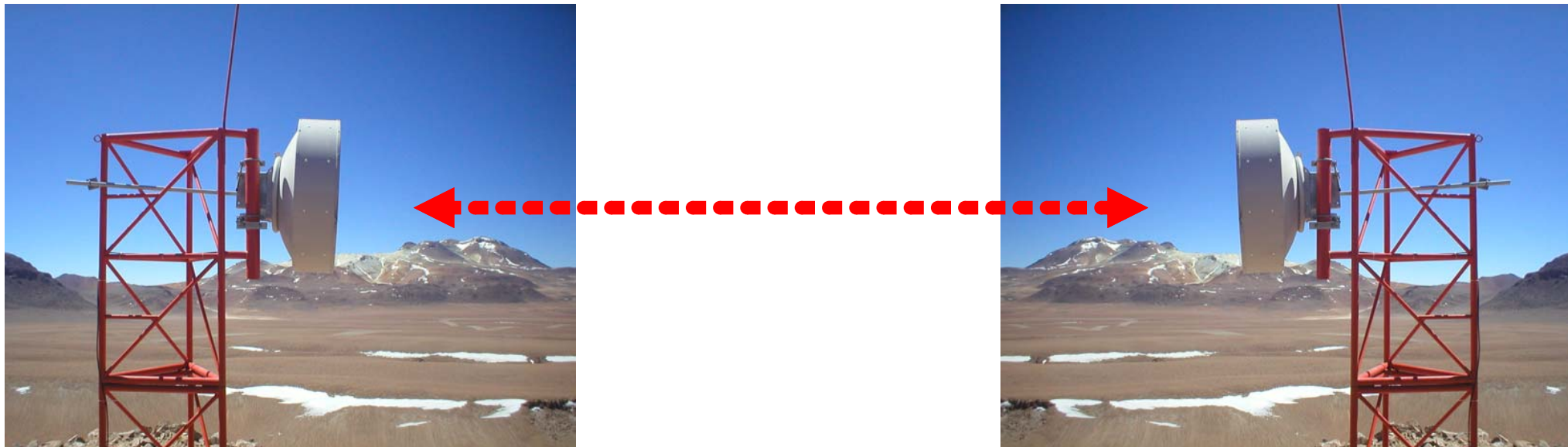


Wireless Topologies

- ▶ Point-to-Point
- ▶ Point-to-Multipoint
- ▶ Mesh Networks

Wireless Topologies: Point-to-Point

A type of network communication where information is sent from a single source to a single destination, or basically communication from one antenna to another.



- ▶ Typical use: connecting 2 points that have Line-of-Sight such as towers, buildings, networks, etc.
- ▶ Free Space Optics (FSO) and Microwave are some types of Point-to-Point technologies depending on the frequency and application.



Point-to-Point Vendors

► Licensed ("Microwave")

- ☐ Alcatel
- ☐ Ceragon
- ☐ Cirronet
- ☐ Dragonwave Systems
- ☐ P-Com
- ☐ DMC Stratex
- ☐ + many more...

► Typical costs \$10,000+ per link

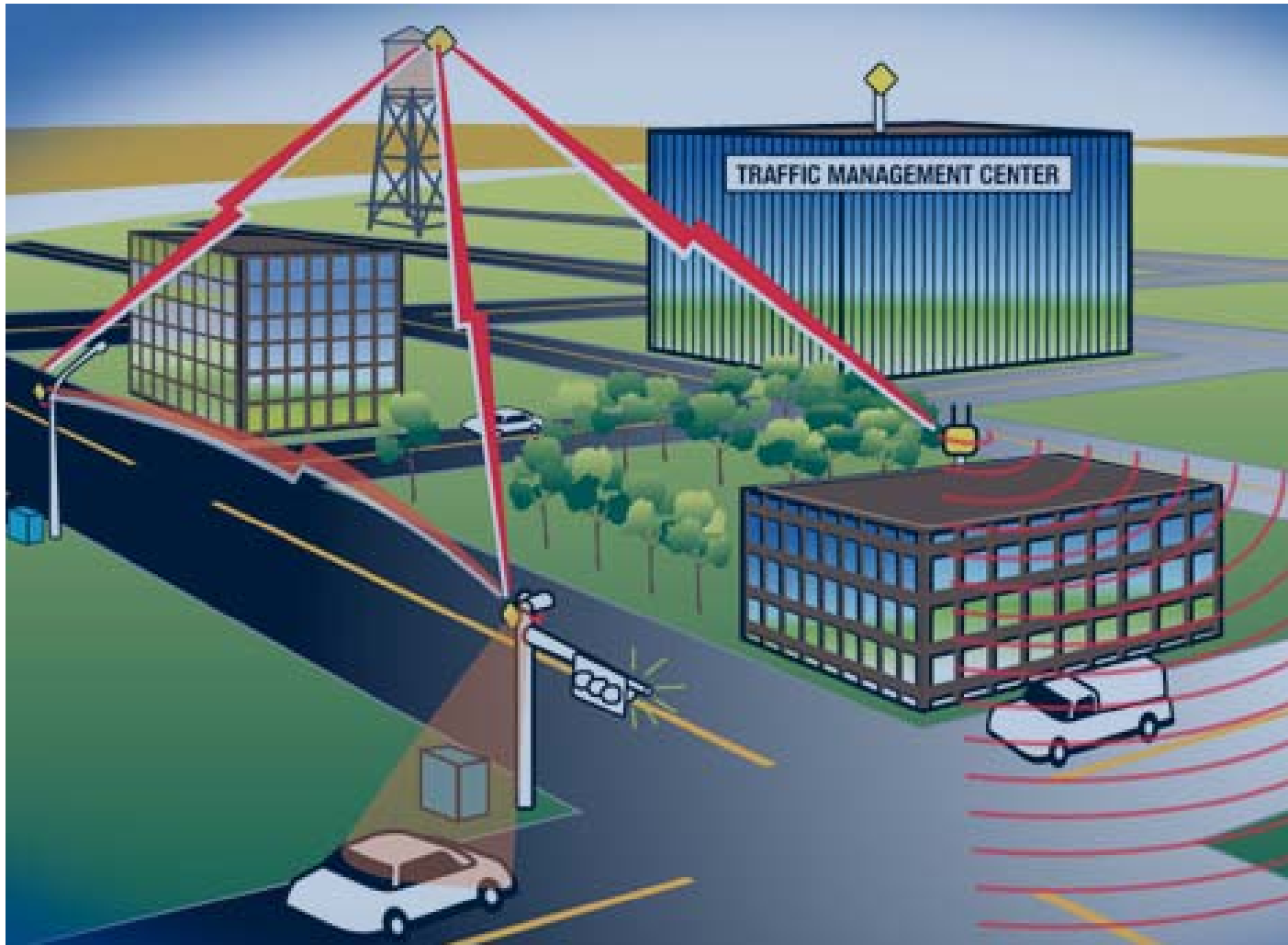
► Unlicensed

- ☐ Gigabeam
- ☐ Motorola
- ☐ Orthogonal Systems (Motorola)
- ☐ Proxim/Terabeam
- ☐ Redline
- ☐ Trango (Atlas)
- ☐ + many more...

► Typical costs \$3,000+ per link

Wireless Topologies: Point-to-Multipoint

- ▶ A type of network communication where information is sent from a single antenna to multiple antennas.





Point-to-Multipoint Components

Access Points (“APs”) – these are the radios that translate the signal from a standard Ethernet (network) signal to a wireless transmission signal and vice-versa.

Antennas – The APs connect to antennas. Each Antenna makes for 1 Sector. A Sector is the “pie piece” of the network coverage.

- ❑ Sectors can be small or large, it really depends on the types of antennas used.
- ❑ Some networks may only need 1 Sector of coverage.

Other Equipment:

- ❑ Router
- ❑ Switch
- ❑ Universal Power Supply (“UPS”)
- ❑ Management Server
- ❑ Equipment Rack
- ❑ Power Distribution Unit (“PDU”)
- ❑ Etc.





Some Point-to-Multipoint Vendors

► Licensed

- ❑ Alvarion
- ❑ Flarion (Qualcomm)
- ❑ IP Wireless
- ❑ Lucent
- ❑ Motorola
- ❑ NextNet (Motorola)
- ❑ Nortel
- ❑ SOMA Networks
- ❑ + many more...

► Unlicensed

- ❑ Alvarion
- ❑ Aperto
- ❑ Motorola
- ❑ Proxim
- ❑ Trango
- ❑ Tranzeo
- ❑ WaveIP
- ❑ WaveRider
- ❑ WiLAN
- ❑ + many more...



Mesh Wireless Elements

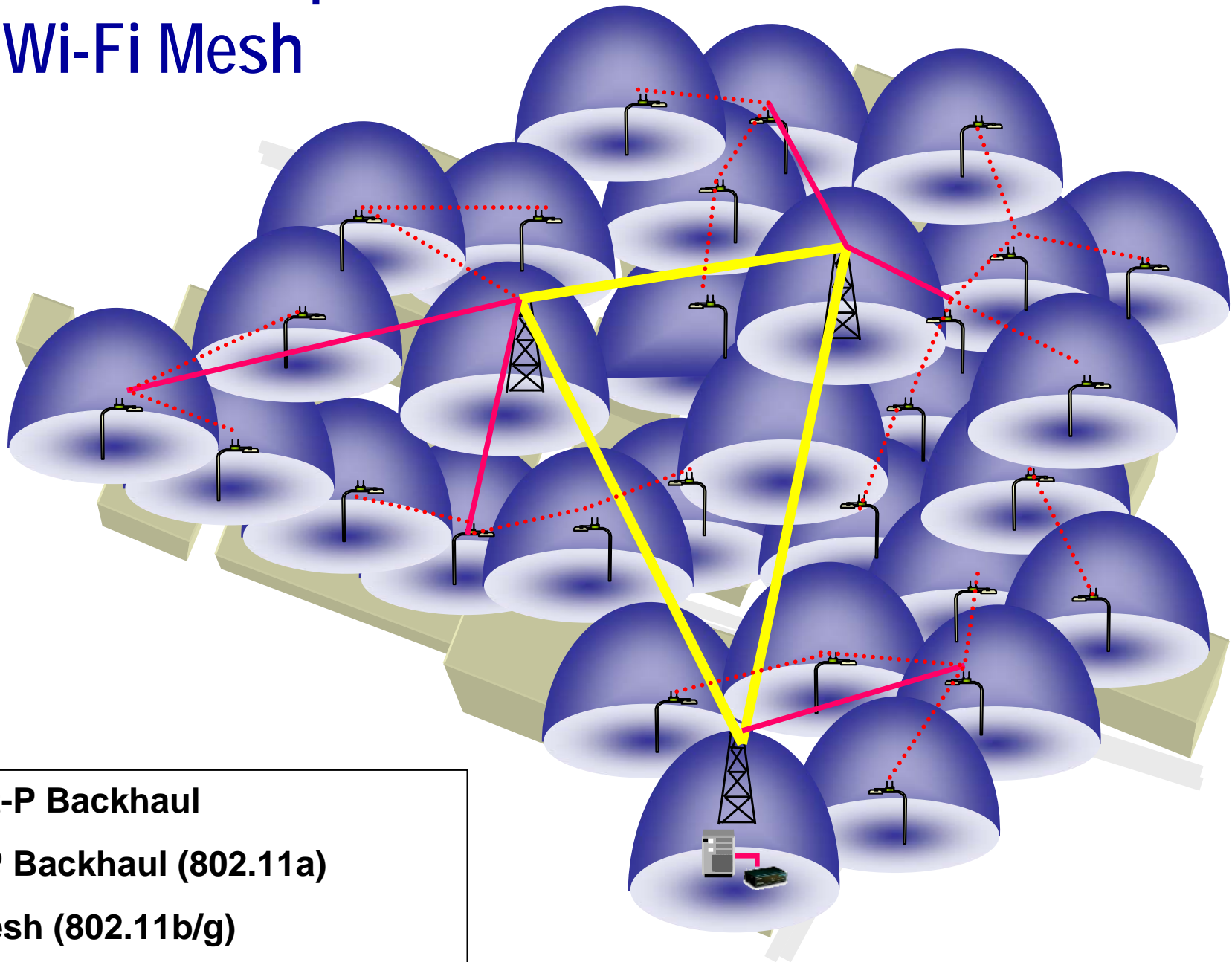
Gateway - the wireless point that mesh nodes attempt to send traffic to access other networks (i.e. the Internet). Gateways may speak to Nodes or Clients.

Node – a node is device that has the ability to speak to other Nodes and Clients and but generally send traffic to only one Gateway . These devices perform a “repeating type function”.

Clients – Devices used by end users to give them access to the mesh.(PCMCIA cards, wireless bridges, etc.)

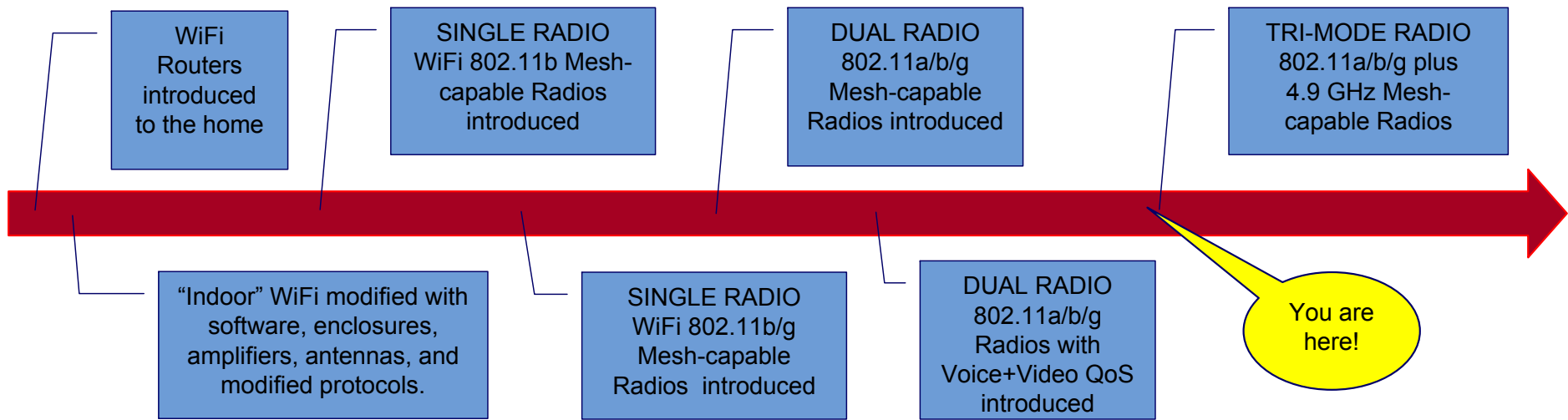


Typical Municipal Wi-Fi Mesh



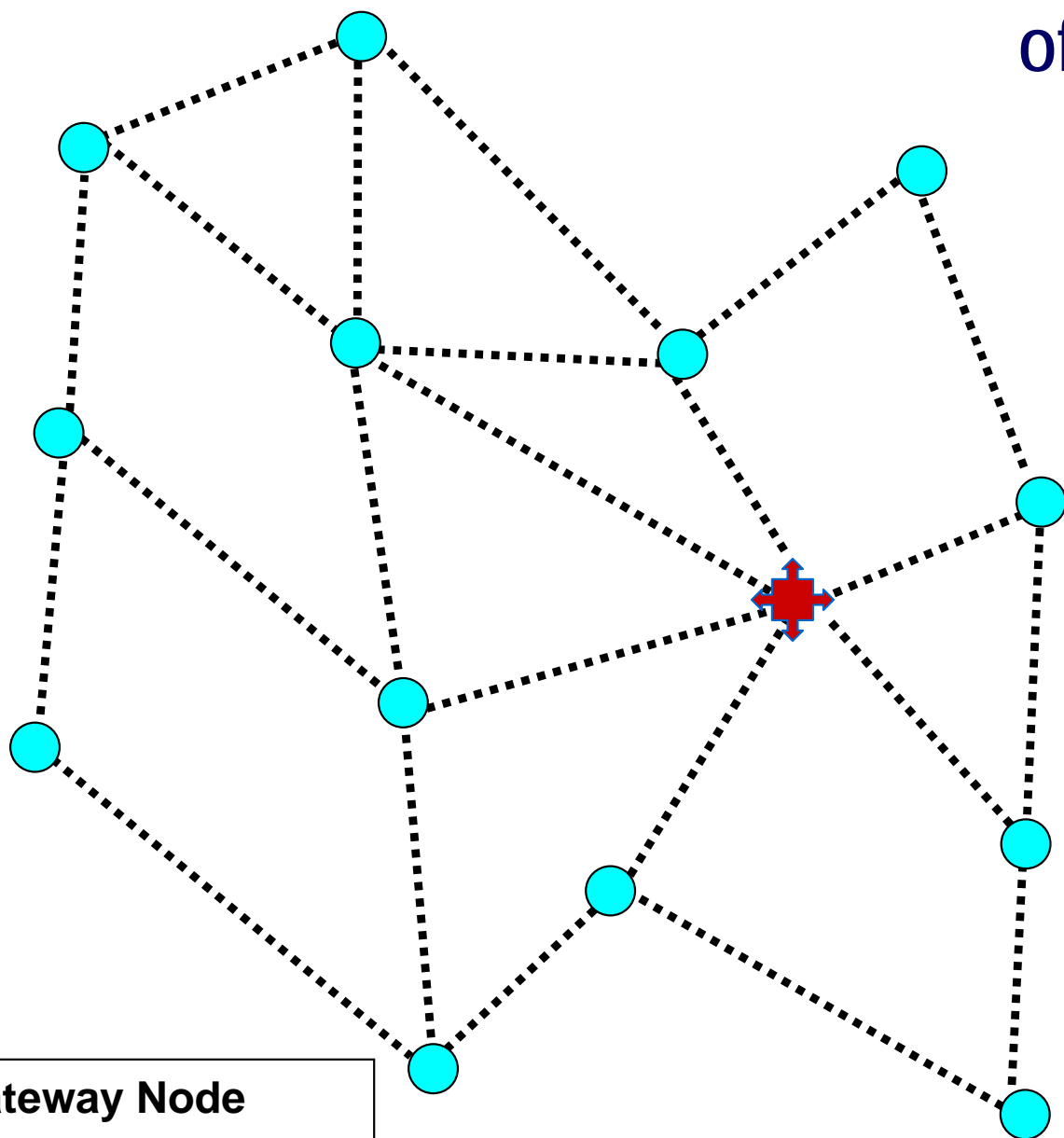


The Evolution of Mesh Networks



- ▶ Future Technologies will include improved range, security, throughput, enhanced QoS, etc.
- ▶ The primary limiting factor is processor and memory capacity in chipset technologies.

Self-Realization of Mesh Networks

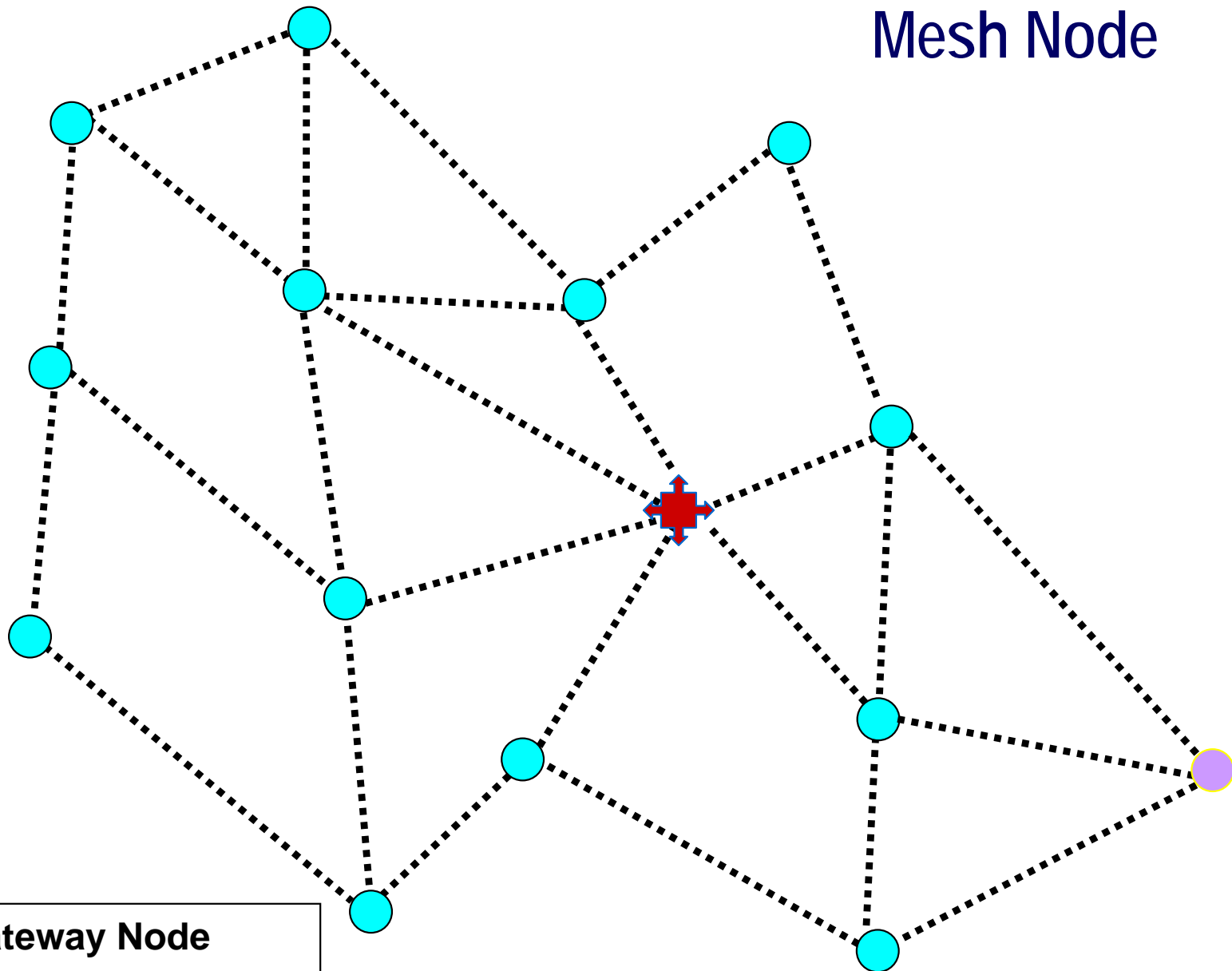


Gateway Node



Mesh Node

Adding a Mesh Node

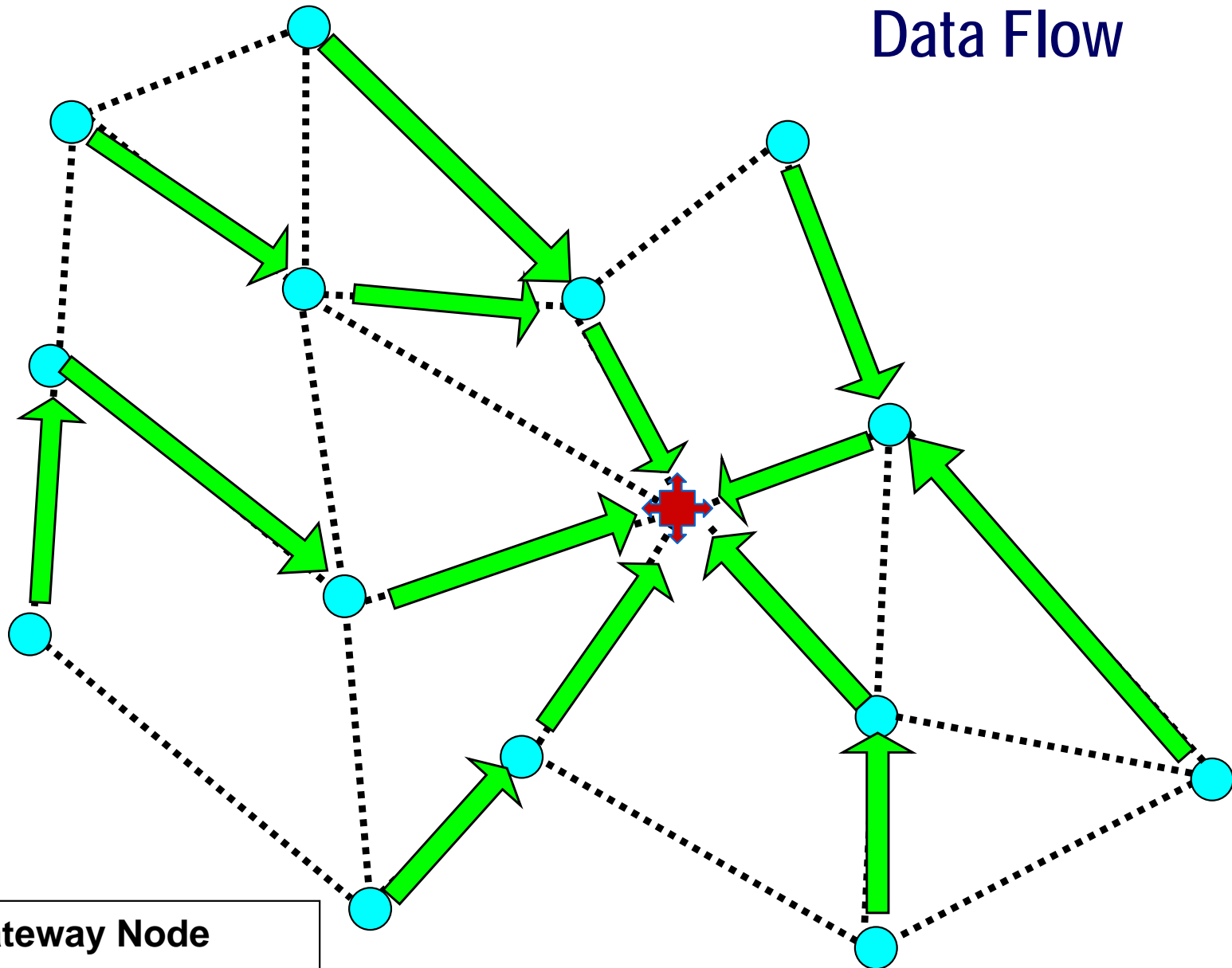


Gateway Node



Mesh Node

Mesh Network Data Flow

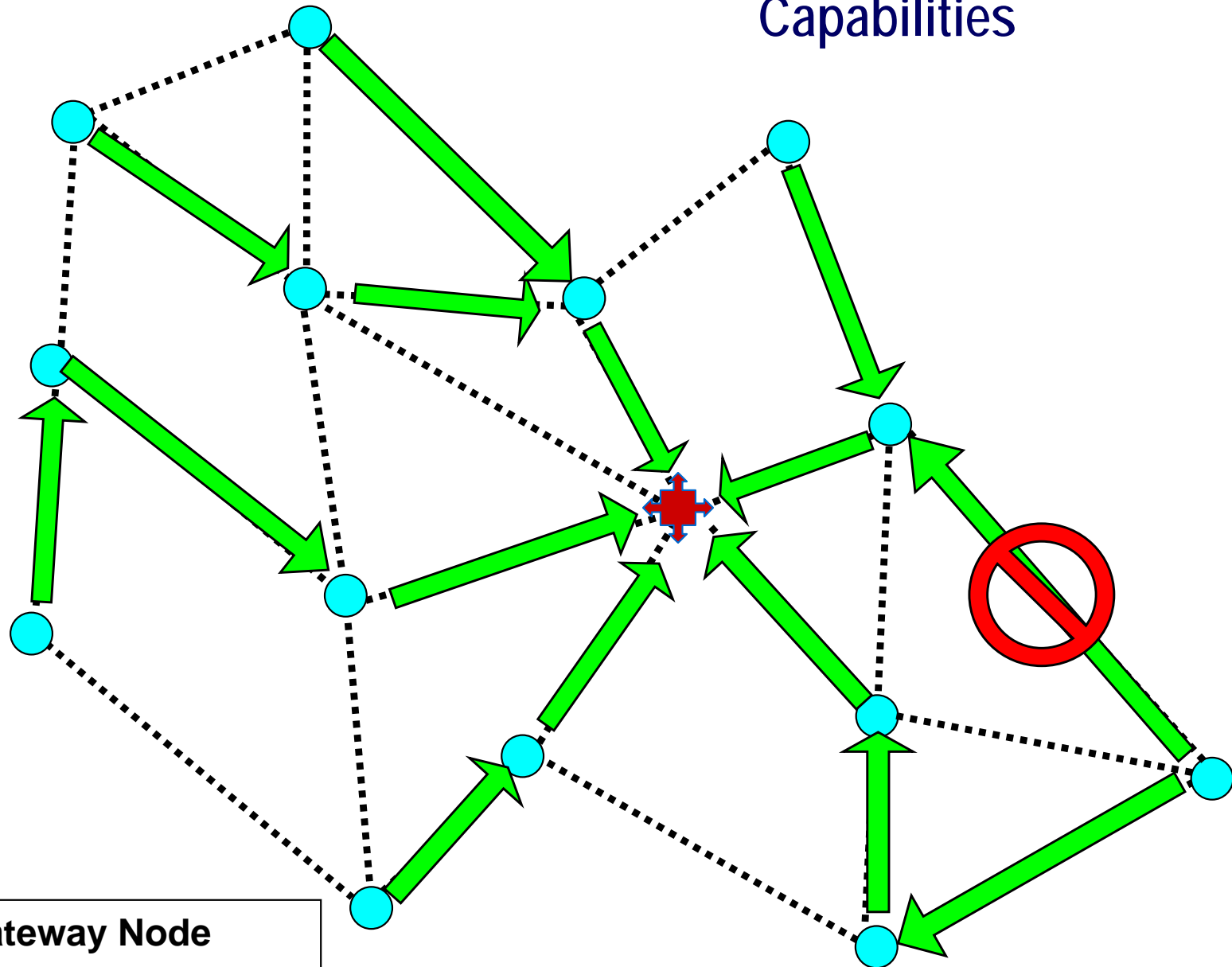


Gateway Node



Mesh Node

Self-Healing "Intelligent" Capabilities

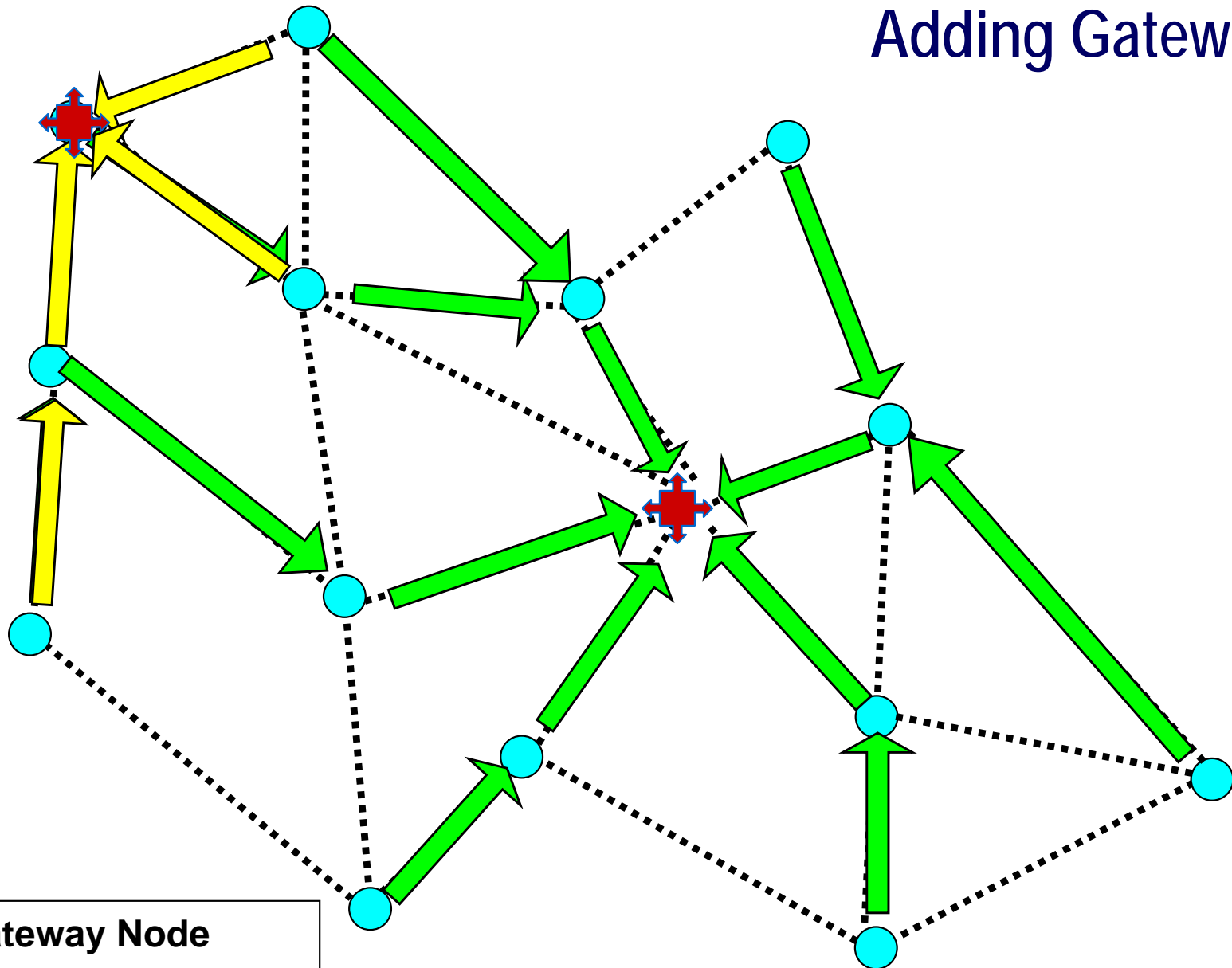


Gateway Node



Mesh Node

Scalability: Adding Gateways



Gateway Node



Mesh Node



Some Mesh Network Vendors

- ▶ BelAir Networks
- ▶ Cisco
- ▶ Go Networks
- ▶ Mesh Dynamics
- ▶ Motorola
- ▶ Nortel
- ▶ Proxim
- ▶ Sensoria
- ▶ SkyPilot
- ▶ Strix Systems
- ▶ Wavion



Start Small – Pilot Networks

- ▶ **The Public Private Partnership model has shifted**
 - ❑ Making the right decisions is more critical
- ▶ **When done right, a Pilot...**
 - ❑ Allows you to determine the true value of applications without making a commitment for millions of dollars.
 - ❑ Allows End Users to play an informed role in shaping the technical direction of your network.
- ▶ **Pilot = “sweet spot”**
 - ❑ Gain decision making information while minimizing risk.



- ⇒ Visit target coverage area, collocation site, determine cable runs, etc.
- ⇒ Identify potential issues

- ⇒ Line-of-Sight Verification
- ⇒ Power Verification
- ⇒ Lat/Long confirmation

- ⇒ Security
- ⇒ IP Architecture
- ⇒ VLAN Requirements
- ⇒ Service Structure
- ⇒ Network Management Structure





Ubiquitous Coverage

- ▶ Given the environmental clutter, networks generally deploy as few as 30 nodes per sq. mile. We've seen as high as 125 in one square mile.
- ▶ Unfortunately finding poles can be a challenge there are a number of forces working against complete coverage.
 - ❑ Those challenges include:
 - ❑ Local Utility rules and regulations
 - ❑ Gang switched light poles
 - ❑ Decorative light pole
 - ❑ Privately owned and operated poles (Home owner association)
 - ❑ No poles
 - ❑ Trees, trees, and more trees
 - ❑ Old infrastructure & lack of documentation
 - ❑ Solar-powered solutions



Mounting Asset Challenges

- ▶ One of the most significant challenges in designing and deploying a WiFi network is identifying appropriate vertical assets for network nodes and backhaul.
- ▶ “Vertical Assets” are buildings, light poles, towers, and terrain suitable for mounting wireless gear and establishing clear Line-of-Sight (“LoS”).





Clear Line of Sight (LOS)

- ▶ Establishing a clear LOS between APs and potential SUs is critical.
- ▶ The unlicensed frequencies that 802.11 a/b/g operate in are highly susceptible to interference (clutter).
- ▶ Additionally, the materials used in construction also affect the ability for the signal to penetrate a facility.



Rule of Thumb for LoS

- ▶ In an outdoor network the signal will lose one (dB) decibel (roughly 50%) of your signal for every 3 meters of tree canopy the signal passes through.
- ▶ When your signal moves through a wall, you will lose roughly 20% of your signal for each wall the signal must penetrate.





Solar-powered Solutions

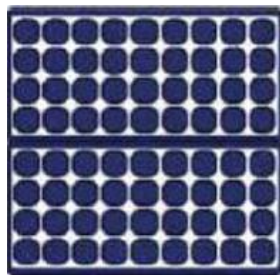
Solar Costs Estimates:

- ❑ New 25' aluminum pole (w/installation, foundation, etc.): \$1,000
- ❑ Solar Panel: \$1,000 ~ \$8,500



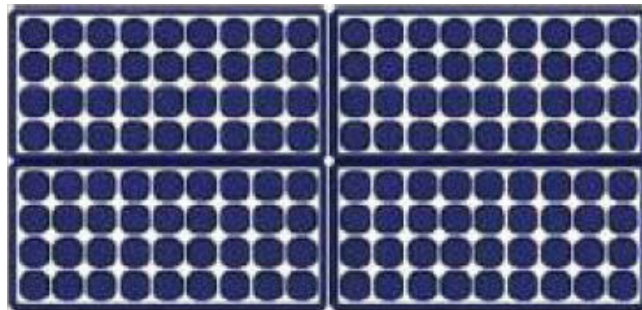
SINGLE SOLAR PANEL

- 5' x 2' solar panel (10 sq. ft.)
- 26 lbs
- 100W @ 12V
- Can support some WiFi Mesh Radios



DOUBLE SOLAR PANEL

- (2) 5' x 2' solar panels (20 sq. ft.)
- 26 lbs * 2 = 52 lbs
- 200W @ 12V, or 100W @ 24V
- Can support some WiFi Mesh Radios along with (1) PtMP CPE



QUAD SOLAR PANEL

- (4) 5' x 2' solar panels (40 sq. ft.)
- 26 lbs * 4 = 104 lbs
- 400W @ 12V, or 100W @ 48V
- Can support any WiFi Mesh Radio along with (1) PtMP CPE

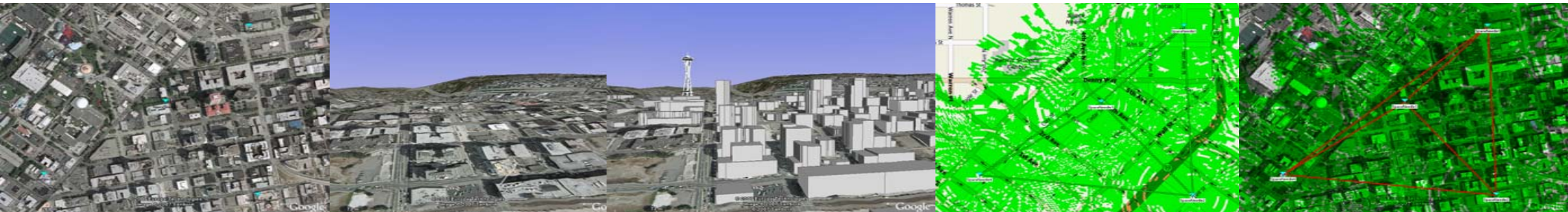
Network Installation and Turnover

Equipment Installation

- ⇒ Equipment Burn-in & Testing
- ⇒ Mesh Radio Installation Management
- ⇒ Bucket Truck Operator Training
- ⇒ Core Network Configuration & Installation

Launch

- ⇒ Drive Test
- ⇒ Develop Coverage Documentation
- ⇒ Provide Network Configurations Documentation



Network Design & Planning may entail a variety of studies to ensure success.



Ongoing Management

Network Monitoring

⇒ Real-time Alarm Monitoring and Alerts

Network Management

⇒ Real-time Performance Optimization

⇒ Proactive Network Care

Network Maintenance

⇒ Equipment management/replacement

Support

⇒ Help Desk Support





Network Maintenance

What Service Levels do I want to maintain?

- ❑ Network Availability (uptime)
- ❑ How do I need to support the Network (8 hours x 5 days, 24x7, "best effort", etc.?)
- ❑ What services do I need to incorporate (Web Hosting, Email, Internet Access, Managed Services, VOIP, etc.?)
- ❑ Commercial Services?

What functions need to be performed?

- ❑ Remote monitoring and maintenance (NOC)
- ❑ Network Administration
- ❑ Field Support
- ❑ Engineering



Models for Maintaining a Network

1. Insource it all

- ❑ The benefit is control.
- ❑ If Network gets large enough, it is more cost effective.
- ❑ Costs much more initially due to training and lack of economies of scale.
- ❑ The million dollar question: *Will your network get big enough?*

2. Outsource all or part

- ❑ The benefits (with the right partner) are cost, efficiency, time to market, and little to no training needed
- ❑ Requires more trust and a solid partnership.
- ❑ Less control over network elements.
- ❑ Not as cost efficient as your network grows

Depending on your Network, Management costs may range between 5% to 35% of the capital cost annually!

The best way to keep these costs down is good planning and good engineering *in advance*.



Network Management Criteria

- ▶ 24x7 Visibility into Network Nodes
 - Alarms to alert when a node is not performing

- ▶ Real-time Equipment Management
 - Visibility into each device

- ▶ Network Health Status

- ▶ Reporting Capabilities
 - Yearly, Monthly, Daily, Hourly

- ▶ Tier 2 & 3 Trouble Ticketing



Top 10 “Lessons Learned”

10. Spectrum Management
9. Unrealistic Expectations
8. Incorrect Equipment Selection
7. Poor Processes
6. Over-confidence
5. Lack of Efficient Operations
4. Poor Design
3. Lack of Clear Objectives
2. Budgets & Business Plan Issues
1. Lack of Expertise & Training



#10 – Spectrum Management

- ▶ Just because you don't need a license to use some spectrum, doesn't mean that you don't have to manage it.
- ▶ Be smart
 - ❑ Even if the equipment you are using claims to have some form of "automatic" channel selection.
- ▶ Do an initial analysis and ensure that it works the way you think it does.
- ▶ Develop a channel plan and attempt to coordinate with other local service providers.
- ▶ Remember the primary cause of interference is "self-interference".



#9 – Unrealistic expectations

- ▶ Many RFPs are being generated with requirements for services and applications that are unrealistic today.
- ▶ Even in the case where applications and services are realistic, many are responding with the wrong equipment.
- ▶ If you generate an RFP, know what you're talking about, hire someone who does or get the training needed.



#8 – Incorrect Equipment Selection

- ▶ This is caused by a lack of expertise and marketing over-hype.
- ▶ Understand what equipment vendors have in common and how their equipment is differentiated.
- ▶ Equipment doesn't all work the same – each have superior qualities in the right environments.
- ▶ Minimum Requirements (Mesh)
 - ❑ Multi Radio
 - ❑ 802.11b/g
 - ❑ 802.11a
 - ❑ 802.11e (QoS)
 - ❑ 802.1Q (VLAN Tagging)
 - ❑ SNMP v3



#7 – Poor Processes

- ▶ An inordinate number of networks are being installed with no processes or poor processes.
- ▶ Are poor processes better than no process as long as they are followed consistently?
- ▶ Process Development is not rocket science (unfortunately).
 - This is experience – pure and simple. Don't let the blind lead the blind.
- ▶ Develop a "Train the Trainer" philosophy.



#6 – Over Confidence

- ▶ *"I installed a Wi-Fi network for my Mom so...I can do this!"*
 - Even a monkey can type Shakespeare if given enough time.
- ▶ Think *Carrier Class*!
- ▶ Don't be afraid to outsource!





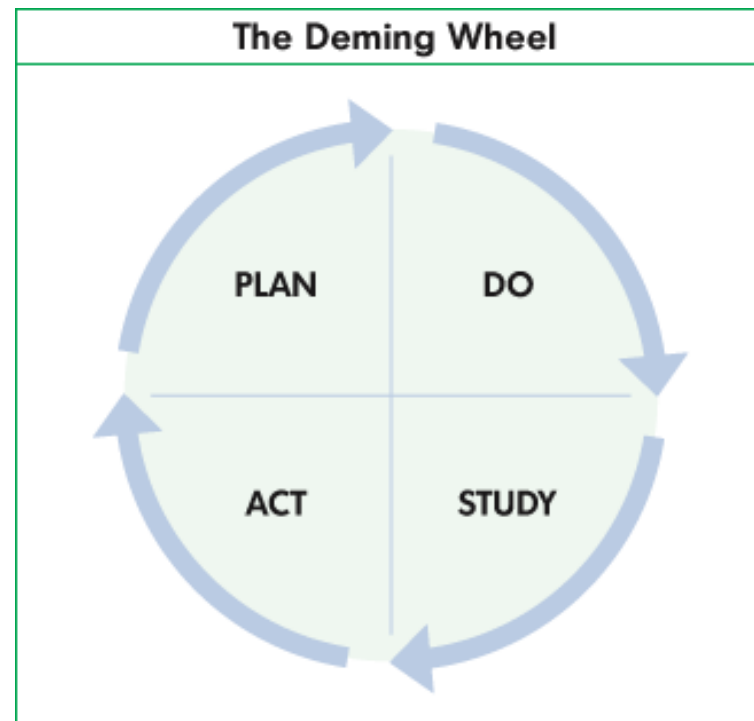
#5 – Lack of Operations

- ▶ A wireless network is dynamic.
 - ❑ We rarely find anyone that has taken the basic steps to monitor their network properly.
- ▶ Few even ask the vendor the right questions.
 - ❑ Don't assume that any vendor's software gives you all the tools and all the answers.
 - ❑ Besides only part of the network is wireless.
- ▶ Questions to ask vendors:
 - ❑ Is everything manageable through SNMP?
 - ❑ ICMP (a.k.a. Ping test) is not enough to understand the health of your network.
Measure and trend and threshold the performance – and assign someone to actively review the data .



#4 – Design and Documentation

- ▶ Concept of TQM (Total Quality Management)
 - ❑ Initially it was difficult to assess the cost of poor quality.
 - ❑ Many existing networks require reverse engineering due to lack of documentation and performance reports.
 - ❑ Do it right the first time. It costs less.





#3 – Lack of Clear Objectives

- ▶ Many want wireless but how many know why, where and what for?
 - ❑ What are the applications?
 - ❑ What are the services?
 - ❑ What security is required?
 - ❑ Do I need to separate traffic?
 - ❑ Who are the users?

- ▶ Start small
 - ❑ Pilot Networks
 - ❑ Gather several layers of data!.



#2 – Poor Budgets and Business Plans

- ▶ We believe in *Budgets and Business Plans* but...
 - ❑ A Model is different from real life.
 - ❑ Again...start small.
- ▶ Remember – Internet access is an application, *not “the application”*.



#1 – Expertise and Training

- ▶ Ensure your people are properly trained or get help.
 - Equipment vendors build equipment not networks.



Summary

- ▶ Start Small
- ▶ Develop minimum requirements
 - ❑ Coverage
 - ❑ Equipment
 - ❑ Services
- ▶ Test your business model
- ▶ Know thy assets!
- ▶ Ensure that you have a Network Operations Plan
- ▶ Ask Lots & Lots & Lots of Questions
- ▶ Ask More Questions

THANK YOU!!!

For more info please contact:

Scott Akrie

CEO

(858) 764-1953

scott@netlogix.com